



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>7</sup> : <b>H04L 9/30</b></p>	<b>A1</b>	<p>(11) International Publication Number: <b>WO 00/42733</b></p> <p>(43) International Publication Date: 20 July 2000 (20.07.00)</p>
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%; vertical-align: top;"> <p>(21) International Application Number: PCT/CA00/00030</p> <p>(22) International Filing Date: 14 January 2000 (14.01.00)</p> <p>(30) Priority Data: 2,259,089                      15 January 1999 (15.01.99)                      CA</p> <p>(71) Applicant (for all designated States except US): CERTICOM CORP. [CA/CA]; 4th floor, 5520 Explorer Drive, Mississauga, Ontario L4W 5L1 (CA).</p> <p>(72) Inventor; and (75) Inventor/Applicant (for US only): LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA).</p> <p>(74) Agents: PILLAY, Kevin et al.; Orange Chari Pillay, Toronto Dominion Bank Tower, Toronto-Dominion Centre, Suite 3600, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).</p> </div> <div style="width: 48%; vertical-align: top;"> <p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p><b>Published</b> <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i></p> </div> </div>		
<p>(54) Title: METHOD AND APPARATUS FOR MASKING CRYPTOGRAPHIC OPERATIONS</p>		
<p>(57) Abstract</p> <p>A method of masking a cryptographic operation using a secret value, comprising the steps of dividing the secret value into a plurality of parts; combining with each part a random value to derive a new part such that the new parts when combined are equivalent to the original secret value; and utilizing each of the individual parts in the operation.</p>		
<pre> graph TD     A[Initialize processor: d, P] --&gt; B[Generate d = Σ bi]     B --&gt; C[Generate random π]     C --&gt; D[Compute d P = Σ (bi ± π) P mod n]           </pre>		
<p><b>200</b></p>		

T00120 65600660